Public Key Infrastructure Analysis

Controlled Substances Ordering System

Certificate Policy

Draft

Prepared for

Drug Enforcement Administration
Office of Diversion Control
Washington, D.C. 20537

April 18, 2002

Prepared by
PEC Solutions, Inc.

Table of Contents

page

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Table of Contents

Section 1 — Introduction

The Drug Enforcement Administration (DEA) regulates the manufacture and distribution of controlled substances in the United States. This regulatory control is designed to prevent the diversion of legitimate pharmaceutical drugs into illegal channels and also to ensure that there is a sufficient supply for legitimate medical uses. The Controlled Substances Ordering System (CSOS) PKI will be operated under the authority of the Drug Enforcement Administration (DEA) Office of Diversion Control Policy Management Authority (PMA). The purpose of the CSOS PKI is to institute the security services of authenticity, integrity and non-repudiation into the DEA's controlled substances electronic ordering system. The Certification Authority (CA) will be governed by the laws of the United States of America and DEA regulations.

End entity (subscriber) certificates will be issued only by the Certification Authority. These subscriber certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating the subscriber is operating under the authority of the DEA CSOS program. *The Certificate and CRL Profile* document, produced under separate cover, provides the necessary guidance for certificate profiles.

This CSOS *Certificate Policy* (CP) is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 2527, *Certificate Policy and Certification Practice Statement Framework.*

The terms and provisions of the CSOS CP shall be interpreted under and governed by applicable Federal and State Law. The United States Government disclaims any liability that may arise from the use of this CSOS CP.

1.1 Overview

A certificate policy is a "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X.509]. This *Controlled Substances Ordering Systems Certificate Policy* has been developed in accordance with IETF RFC 2527.

This document, along with the *Certificate and CRL Profile* document, define the creation and management of certificates for use in electronic ordering applications. The associated Certification Practices Statement (CPS) describes the practices of the CSOS CA. It will be used to establish the level of assurance and trust that can be placed in the authenticity and integrity of the public keys contained in certificates that are issued by the CSOS CA. The word "assurance" used in this CP indicates to what extent a relying party

can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate.

This Certificate Policy specifies: (1) the Certification Authority, the subscribers, and the relying parties authorized to participate in the PKI program described by this Policy, (2) the obligations of the participants governed by this Certificate Policy, and (3) the minimum requirements for the issuance and management of digital certificates that are used in verifying transactions and digital signatures in CSOS.

1.2 Identification

This Certificate Policy is registered with the National Institute of Standards and Technology (NIST). The object identifier (OID) assigned to this CP is dea-csos-cp ::= { 2.16.840.1.101.3.2.1.9.1}.

All CSOS Certificates issued under this Policy shall reference this Policy by including the appropriate OID for this Policy in the Certificate Policies field of the CSOS Certificate. The foregoing OID may not be used except as specifically authorized by this Policy.

1.3 Community and Applicability

The following sections discuss the roles relevant to the administration and operation of the DEA CSOS PKI.

1.3.1 Certification Authority (CA)

The DEA CSOS Certification Authority will be established by the DEA. It will be operated and maintained by the DEA or by an authorized DEA contractor. The DEA CSOS Certification Authority is authorized to issue and manage certificates in accordance with the terms and conditions specified within this Certificate Policy.

1.3.2 Registration Authority (RA)

The CSOS CA shall perform both the role and the functions of a Registration Authority (RA). The RA will process applications of CSOS subscribers and operate according to the stipulations of this Certificate Policy.

1.3.3 Subscribers (all who transmit electronic orders)

A subscriber is the entity whose name appears as the subject in a certificate issued by the DEA CSOS CA, who attests that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate. CSOS subscribers are limited to DEA employees, authorized Department of Justice (DOJ) officials, approved registrants, holders of Powers of Attorney (POAs) and properly cleared and approved contractor personnel.

1.3.4 Relying Parties (all who accept electronic orders)

A relying party is the entity who, by using a subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message, and relies on the validity of the public key bound to the subscriber's name. The relying party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The relying party must use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.

1.3.5 Applicability

CSOS subscriber certificates shall only be issued to entities engaged in the transfer of controlled substances between manufacturers, distributors, retail pharmacies, authorizing institutions and other registrants and must be used for the signing of electronic transaction orders, however the use of CSOS certificates is not restricted to this single application.

1.4 Contact Details

1.4.1 Specification Administration Organization

The DEA, Office of Diversion Control is responsible for all aspects of this Certificate Policy.

1.4.2 Contact Person

Chair, Policy Management Authority
Drug Enforcement Administration
Office of Diversion Control
Washington, D.C. 20537

1.4.3 Person Determining CPS Suitability for the Policy

The CSOS Policy Management Authority (PMA) shall approve the Certification Practices Statement of the CA. The CA will be required to periodically attest to the compliance of the CPS as set forth in this Certificate Policy.

Section 2 — General Provisions

This section specifies any applicable presumptions on a range of legal and general practice topics.

2.1 Obligations

2.1.1 CA Obligations

The CA will shall conform to the stipulations of this document including:

- Protect the CA's private signing key in accordance with this Certificate Policy;
- Sign certificates only after verifying the identify of the certificate subject in accordance with Section 3 of this Certificate Policy, and that the subject holds the private key corresponding to the public key in the certificate;
- Use the private signing key only when issuing certificates or signing Certificate Revocation Lists (CRL) which conform to this Certificate Policy;
- Provide to the PMA a CPS, as well as any subsequent changes, for conformance assessment;
- Conform to the stipulations of the approved CPS;
- Include only valid and appropriate information in the certificate, and maintain evidence that due diligence was exercised in validating the information contained in the certificate;
- Ensure that subscribers are informed of their obligations as defined in Section 2.1.2, and informed of the consequences of not complying with those obligations;
- Revoke the certificates of subscribers found to have acted in a manner counter to those obligations;
- Provide for the renewal of certificates;
- Operate or provide for the service of a repository for maintaining subscriber certificate information and status;
- Accurately publish certificates and Certificate Revocation Lists (CRLs), processing certificate applications and responding to revocation requests in a timely and secure manner in accordance with Section 4.4.4;

- Maintain records necessary to support requests concerning its operation, including audit files and archives.

2.1.2 Subscriber Obligations

In all cases, prior to releasing or publishing a CSOS Certificate, the CA shall ensure that the subscriber named in the CSOS Certificate has signed a Subscriber Agreement agreeing to be bound by this Certificate Policy as a subscriber and obligating the subscriber to:

- Protect their private key in accordance with this Certificate Policy and as stipulated in their certificate acceptance agreement, taking all reasonable measures to prevent its loss, disclosure, modification, or unauthorized use;

- Acknowledge that by accepting the certificate, the subscriber is warranting that all information and representations made by the subscriber included in the certificate are true;

- Use the certificate only for authorized and legal purposes, consistent with this Certificate Policy;

- Notify the CA in a timely manner if they suspect that their private key is compromised or lost;

- Abide by all terms, conditions, and restrictions levied upon their use of the private keys and certificates.

2.1.3 Relying Party Obligations

Relying parties are responsible for performing checks for validity of each digitally signed transaction as required by applicable federal and state regulations. Relying parties are responsible for examining the Certificate Policy to understand all of their rights and obligations under the Certificate Policy.

2.1.4 Repository Obligations

The CA shall ensure that there is a repository where CSOS PKI certificates are published and available to validate signatures. The repository shall be an X.500 compliant directory with Lightweight Directory Access Protocol (LDAP) access. The CA shall assert a high level of reliability and availability of the repository. This CP must be published in the repository. CRLs must be published in accordance with requirements stated in Section 4.4.6 of this Certificate Policy.

2.2 Liability

2.2.1 CA Liability

The CA disclaims any liability of any kind whatsoever for any award, damages, or other claim or obligations of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon, a CSOS PKI certificate or its associated public/private key pair.

2.3 Financial Responsibility

2.3.1 Indemnification by Relying Parties

The CA assumes no financial responsibility for improperly used subscriber certificates.

2.3.2 Fiduciary Relationships

No Stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the United States of America and the laws of the states in which the subscriber and relying party are domiciled shall govern the enforceability, construction, interpretation, and validity of this Certificate Policy.

2.4.2 Severability, Survival, Merger, Notice

Should it be determined that one section of this Certificate Policy is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this Certificate Policy are described in Section 8.

2.4.3 Dispute Resolution Procedures

The PMA shall resolve any dispute arising out of this Certificate Policy or the CPS unless precluded by governing law or other agreement.

2.5 Fees

The CA shall not impose any fees to end entities for the reading of this Certificate Policy, its CPS, or any other document incorporated by reference. The CA may charge fees for the issuance of certificates as well as for access to certificates or certificate status information, subject to agreement between the CA and the subscriber and/or between the CA and the relying party, in accordance with a fee schedule published by the CA in its CPS.

2.6 Publication and Repository

2.6.1 Publication of CA Information

The CA shall publish the following information to either an online repository or a web site that is available to subscribers and relying parties:

- Certificates that reference this Certificate Policy;
- A Certificate Revocation List (CRL);
- The CA's certificate;
- A copy of this Certificate Policy, including any waivers granted to the CA by the PMA.

2.6.2 Frequency of Publication

All information to be published in the repository shall be published promptly after such information becomes available to the CA. Certificates shall be published following subscriber. Certificate revocation information shall be published as specified in Section 4.4.6. The CA shall specify the frequency of publication for various types of information within its CPS.

2.6.3 Access Controls

The information in the CSOS directory will be publicly available through the Internet. There shall be no access controls on the reading of this Certificate Policy. There shall be appropriate access controls restricting who can write or modify policies, certificates, certificate status or CRLs.

2.6.4 Repositories

The location of the CSOS repository shall be appropriate to the certificate-using community, and in accordance with the CPS.

2.7 Compliance Audit

The CA shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the CPS are implemented and enforced.

2.7.1 Frequency of Entity Compliance Audit

The CA shall undergo a compliance audit to demonstrate compliance with this Certificate Policy and the CSOS CPS. Re-certification will be required no less than once per year. The PMA reserves the right to conduct periodic and unscheduled compliance audits or

inspections of the CA to validate that it is operating in accordance with the security practices and procedures described in the CPS.

2.7.2 Identity/Qualifications of Auditor

The person or entity seeking to perform a compliance audit must be qualified to perform an American Institute of Certified Public Accountants (AICPA) audit and must be thoroughly familiar with requirements that the PMA defines for the issuance and management of CSOS certificates as provided in this Certificate Policy.

2.7.3 Auditor's Relationship to Audited Party

The compliance auditor and the CA shall have sufficient organizational independence to ensure an unbiased, independent, and repeatable evaluation.

2.7.4 Topics Covered by Audit

The purpose of the compliance audit shall be to verify that the CA has a system in place to assure that its operational policies and procedures are consistent with the requirements stated in this Certificate Policy and its Certificate Practices Statement.

2.7.5 Actions Taken as a Result of Deficiency

Should the compliance auditor find a discrepancy between the CA's operation and the stipulations contained in the CP or CPS, the following must occur:

- The compliance auditor shall note the discrepancy;
- The compliance auditor shall notify both the PMA and Operations Management Authority (OMA) of the results of the audit in writing;
- The PMA shall determine what further actions are necessary pursuant to the requirements of this CP to correct any discrepancies and shall proceed to take such corrective actions without delay.

2.7.6 Communication of Results

If the CA is found to be non-compliant with the CPS or this Certificate Policy, the PMA shall be immediately notified by the OMA at the completion of the audit. Required remedies shall be defined and communicated to the CA as soon as possible to limit the risks identified. A list of recommended remedies shall be communicated to the appropriate authority.

2.8 Confidentiality

The CA shall keep all subscriber information confidential with the exception of information that is included in the certificate. The subscriber information shall be used only for the purpose collected and such information shall not be released without the prior written consent of the subscriber, unless otherwise required by law. Information released to law enforcement officials shall be in accordance with applicable laws and regulations. Any request for release of subscriber information shall be authenticated.

2.9 Intellectual Property Rights

Private keys shall be treated as the sole property of the legitimate holder of the corresponding public key identified in the CSOS certificate.

Section 3 — Identification and Authentication

3.1 Initial Registration

Subscribers shall enter into a binding agreement with the CSOS CA and submit a notarized application. The CA is responsible for verifying the identity and authorization of the subscriber through the DEA's Controlled Substance Act (CSA) database. CSOS subscribers shall be DEA registrants who are listed in the CSA database or holders of a valid power of attorney. The PMA will ensure that CSA database information is readily available for verification.

3.1.1 Types of Names

Names of certificate subjects must be X.500 Distinguished Names (DN). The Legal Name (LN) must be the same as that listed on the DEA Registration for registrants or the same as that listed on the letter granting Power of Attorney (POA) for holders of POA. For registrants, the LN must correspond to entries presented in the CSA database.

3.1.2 Need for Names to be Meaningful

The subject name listed in a certificate shall identify the person to whom it is assigned in a meaningful way, representing the subscriber in a way that is easily understandable for humans.

3.1.3 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are established by the PMA. These rules are contained in the *Certificate and CRL Profile* document.

3.1.4 Uniqueness of Names

The distinguished name (DN) shall be unique for each subscriber.

3.1.5 Name Claim Dispute Resolution Procedure

The PMA shall resolve any name collisions that are brought to its attention.

3.1.6 Recognition, Authentication and Role of Trademarks

Certificate subject names issued under this Certificate Policy shall be chosen by the CA. The CA is not obligated to research trademarks or resolve trademark disputes. The CA may refuse to accept a name known to be a trademark of someone else, or deemed inappropriate for use in the certificate.

3.1.7 Method to Prove Possession of Private Key

The subject named in a certificate shall be required to prove possession of the private key, which corresponds to the public key in the certificate request, in accordance with the Certificate Practices Statement.

3.1.8 Authentication of Organization Identity

This Certificate Policy applies solely to personal certificates. The CA shall not issue certificates to organizations (as opposed to individuals) referencing the OID of this Certificate Policy.

3.1.9 Authentication of Individual Identity

Subscribers shall submit the following information/credentials to the CA for identity verification:

- Two copies of identification, one of which must be a government-issued photo ID, such as a driver's license or passport;
- A copy of a current DEA registration certificate (form 223) of the applicant (or the applicant's employer for POA holders);
- A letter, on company letterhead, certifying current employment by the registrant. The letter must include the applicant's current work mailing address, work telephone number, and work e-mail address;
- A signed Subscriber Agreement stating that the applicant has read and understands the terms of this Certificate Policy and has agreed to the statement of subscriber obligations that the CA provided;
- For individuals with power of attorney (POA) to sign orders, a copy of the power of attorney;
- For POAs, a signed Subscriber Agreement from the registrant indicating that the registrant has read and agreed to the statement of registrant obligations that the CA provided.

The CA shall verify the subscriber's identity by crosschecking application information with relevant information from the CSA database.

3.2 Routine Re-key

The CA shall notify the subscriber 45 days prior to the expiration date of the subscriber's CSOS certificate. The subscriber may request that the CA issue a new CSOS certificate for a new key pair, provided that the original certificate has not been revoked and the

subscriber is in good standing with the CA, continuing to qualify as a DEA registrant or POA, as defined in Section 1.3.3. Such a request may be authenticated on the basis of the subscriber's digital signature using the current private key for a total of 2 certificate renewals. Upon the third renewal request, subscribers shall be required to establish identity using the initial registration process described in Sections 3.1.9 and 4.

3.3 Re-key after Revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the subscriber go through the initial registration process as described in Sections 3.1.9 and 4.

3.4 Revocation Request

Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised. Revocation request procedures are described in Section 4.4.3.

Section 4 — Operational Requirements

4.1 Certificate Application

All subscriber applicants shall submit a completed application in accordance with Section 3.1.9, entering into an initial agreement with the CA. Upon successful completion of the subscriber identification and authentication process in accordance with this Certificate Policy, the applicant shall generate a key pair and demonstrate that it is a functioning key pair as defined in the CPS. The private key must be protected against compromise.

4.2 Certificate Issuance

Upon successful completion of the subscriber identification and authentication process in accordance with this Certificate Policy, and approval of the certificate application, the CA shall notify the applicant. The CA shall make the certificate application authorization code and password available to the applicant for receipt by the approved certificate applicant only.

4.3 Certificate Acceptance

By accepting a CSOS certificate, the subscriber acknowledges that all information contained in the certificate is accurate and reaffirms that he or she agrees to the terms and conditions contained in this Certificate Policy definition and the CPS.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subscriber and the subscriber’s public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate become invalid;
- Privilege attributes asserted in the subscriber's certificate are reduced;
- It can be demonstrated that the subscriber has violated the stipulations of the Subscriber Agreement;
- The private key is lost or compromise is suspected;
- The subscriber or other authorized party (as defined in the CA's CPS) asks for his/her certificate to be revoked.

4.4.2 Who Can Request Revocation

The persons permitted to request revocation of a CSOS certificate issued pursuant to this Certificate Policy are the subscriber, the subscriber's sponsor, and the PMA.

4.4.3 Procedure for Revocation Request

A certificate revocation request shall identify the certificate to be revoked and provide the reason for its revocation. Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties. All revocation requests shall be authenticated. Electronic requests shall be authenticated using the digital signature of the requestor. Revoked certificates shall be identified in CRLs, which are posted to the CA repository.

4.4.4 Revocation Request Grace Period

When a key compromise is detected, suspected, or when discovered risk is determined to warrant revocation, the revocation request shall be submitted within 6 hours of such an event. The CA shall publish in its CPS the maximum time within which it will process revocation requests resulting from other reasons.

4.4.5 Circumstances for Suspension

No Stipulation.

4.4.6 CRL Issuance Frequency

Within 18 hours of receiving a valid revocation request, the CSOS CA shall revoke the subject certificate and publish an updated CRL. In the event of key compromise or loss, CRLs containing the newly revoked certificate information shall be published within 6 hours of notification. The CSOS CA shall issue CRLs within a period not to exceed *24-hours/7 days a week.*

4.4.7 CRL Checking Requirements

Relying parties must validate every CSOS certificate received in connection with a transaction through valid and unexpired CRLs as required by applicable federal and state regulations. CSOS certificates shall include pointers to CRLs identified in the certificate's **cRLDistributionPoints** extension field.

CRLs may be cached, relied upon and utilized until they expire unless otherwise notified by the PMA.

4.4.8 Other Forms of Revocation Advertisements Available

No Stipulation.

4.4.9 Checking Requirements for Other Forms of Revocation Advertisements

See section 4.4.7.

4.5 CA Security Audit Procedures

For audit purposes, the CA will log operational events pertaining to subscriber enrollment and certificate management. The specific procedures for auditing the system will be stated in the CPS.

4.5.1 Types of Events Recorded

Auditable events include, but are not limited to the:

- Key life cycle management;
- Certificate life cycle management;
- Cryptographic device life cycle management;
- Entry of applicant information;
- Security sensitive events.

Auditable event entries, both automatic and manual, shall contain the date and time, sequence number, nature of entry, source of entry, and identity of entity making the entry. Procedures specifying integrity controls, event record lifetime and event record access shall be implemented and maintained. The audit log should be reviewed for abnormalities in support of any suspected violation and for events such as repeated failed actions, requests for privileged information, attempted access of system files, and certificate and revocation requests that fail authentication and validation criteria. A review of event entries must be done regularly and follow up actions must be taken for suspicious events or omissions.

4.5.2 Frequency of Processing Log

The Operations Manager shall review audit logs. All significant and notable events affecting the security of the CSOS system shall be addressed at least once a month.

4.5.3 Retention Period for Audit Log

Audit logs shall be retained for operational and archival purposes. For operational purposes, the audit logs shall be retained onsite until completion of processing stipulated

in Section 4.5.2. Security audit data shall be retained as archive records in accordance with Section 4.6.

4.5.4 Protection of Audit Log

CA system configuration and procedures must be implemented together to ensure that only authorized persons read, archive or delete security audit data. The entity performing security audit data archive need not have modify access, but procedures must be implemented to protect archived data from disclosure, deletion or destruction prior to the end of the security audit data retention period.

4.5.5 Audit Log Backup Procedures

Adequate backup procedures must be in place to comply with archive requirements identified in Section 4.6 and to recover audit log data in the event of a system failure.

4.5.6 Audit Collection System (Internal vs. External)

No Stipulation.

4.5.7 Notification to Event-Causing Subject

No Stipulation.

4.5.8 Vulnerability Assessments

Vulnerability assessments must be conducted at least quarterly and after any configuration changes to identify potential vulnerabilities or events that would affect the integrity and operation of the CA.

4.6 CA Records Archival

4.6.1 Types of Events Recorded

The following data and files shall be archived by the CA:

- All computer security audit data;
- All certificate application data;
- All CSOS certificates, CRLs and certificate status records generated;
- CA key histories;
- The CSOS Certification Practices Statement.

4.6.2 Retention Period for Archive

Archival of the recorded events in Section 4.6.1 shall be retained and protected against modification or destruction for a period as specified in the CPS, to exceed ten years, 6 months.

4.6.3 Protection of Archive

The media that the archive is stored on must be protected from modification and destruction either by physical security alone, or by a combination of both physical security and cryptographic protection. It should also be provided adequate protection from environmental threats such as temperature, humidity and magnetism.

4.6.4 Archive Backup Procedures

Adequate backup procedures must be in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

4.6.5 Requirements for Time-Stamping of Records

No Stipulation.

4.6.6 Archive Collection System (Internal or External)

Archive data may be collected in any expedient manner.

4.6.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, verify, package, transmit, and store CA archives shall be published in the CA's CPS. Only those authorized shall be permitted to access the archive.

4.7 Key Changeover

To minimize risk from compromise of the CA's private signing key, that key may be changed. After changeover, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate must be available to verify old signatures until all of the certificates signed using the associated private key have also expired.

The CA key must be changed while sufficient life remains on the key to allow uninterrupted validity of all subscribers. If the key must be changed due to changes in software or hardware, the current key must be maintained for a sufficient period to allow uninterrupted validity of all subjects. New keys shall be generated as per Section 3.2.

4.8 CA Compromise and Disaster Recovery

4.8.1 Disaster Recovery

The CA shall have in place an appropriate disaster recovery/business resumption plan that is capable of resuming services in accordance with this Certificate Policy.

Recovery/resumption plans must be in place for all potential scenarios (e.g. inadvertent destruction/corruption of critical systems/data, natural disaster, and terrorism) recognized in a current risk assessment. The CA must identify redundant capabilities (e.g. back-up systems, location of archived data, records/key availability, and off-site facilities/personnel). A list of key personnel and their contact information must be easily accessible in the event of an emergency.

4.8.2 Key Compromise Plan

The CA must have in place an appropriate key compromise plan that defines the procedures that will be followed in the event of a compromise of the private signing key used by the CA to issue certificates. Such a plan shall include procedures to revoke all affected CSOS certificates within 24 hours of discovering the key compromise and procedures that allow for the prompt notification of all subscribers and known relying parties. The plan shall also include procedures for the prompt re-issuance of valid certificates.

4.9 CA Termination

In the event that the CSOS CA terminates operations, the PMA shall oversee the termination process. The CA shall notify all Subscribers of the CSOS CA cessation of operation. All certificates issued by the CSOS CA shall be revoked.

Section 5 — Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

Physical security controls shall be implemented that protect the CA hardware and software from unauthorized access and damage. CA cryptographic modules shall be protected against theft, loss, and unauthorized use. The CA shall implement appropriate physical security controls to restrict access to the hardware and software (including the server, workstations, and any external cryptographic hardware modules or tokens) used in connection with providing authorized CA services. Proper physical barriers shall be in place. For instance surrounding walls shall extend from real ceiling to real floor not raised floor to suspended ceiling. The facility will be locked and intruder detection systems will be activated while the facility is unoccupied. Fire prevention and protection controls will be in place including a fire extinguisher system. CA facilities must be constructed so as to prevent exposure of systems to water. All electronic physical security devices will be tested daily.

The CA equipment shall consist of equipment dedicated to the CSOS CA function; it shall not perform non-CA related functions. The CA's facility shall also store backup and distribution media in a manner sufficient to prevent loss, tampering, or unauthorized use of the stored information.

5.1.2 Asset Classification and Management

Inventory records must be generated and maintained for all equipment used to support CA operations. Classification of this equipment according to its function and media is required. Assignment of responsibility for each piece of equipment to individuals is also required maintaining a chain of custody.

5.1.3 Physical Access Controls

The CA facility’s main entrance shall be attended during normal working hours. During non-working hours the main entrance shall be controlled by electronic access control devices. Physical access to the CA’s systems will be limited to authorized individuals with a valid purpose to enter. Authentication controls will be used to access areas containing the CA’s systems. Visible identification shall be worn while at all times while in the confines of the CA. Those persons not authorized to enter the facility but who require access for business purposes, can enter the facility, only if an authorized CSOS manager or member of the operations staff escorts them. Their arrival and departure must be recorded. Visitors working unsupervised in the area of the CA’s systems are prohibited.

All access to the facility must be logged. CA equipment shall always be protected from unauthorized access. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated.

The physical security requirements pertaining to the CA are:

- Ensure that no unauthorized access to the CA is permitted;
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers;
- The facility shall be manually or electronically monitored for unauthorized access and intrusion at all times;
- Ensure an access log is maintained and inspected daily.

A security check of the facility housing the CA equipment shall occur prior to leaving the facility unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation;
- Security containers are properly secured;
- Physical security systems are tested and functioning properly;
- The area is secured against unauthorized access.

An access policy detailing the procedures for physical access shall be maintained and reviewed periodically.

5.1.4 Power and Air Conditioning

The CA facility shall be supplied with power and air conditioning sufficient to create a reliable operating environment. Personnel areas within the facility shall be supplied with sufficient utilities to satisfy operational, health, and safety needs.

5.1.5 Cabling and Network Devices

Cabling and network devices supporting CA services shall be protected from interception and damage.

5.1.6 Media Storage, Handling, Destruction, and Reuse

CA storage media and devices containing storage media shall be checked to ascertain if they contain sensitive data prior to disposal or reuse. Items found to contain sensitive information will be physically destroyed or securely overwritten at least twice, using a

disk formatting utility designed especially for the permanent removal of data from media. Items whose contents cannot be determined will be physically destroyed. Storage media used by the CA shall be protected from environmental threats of temperature, humidity and magnetism.

Removable cryptographic modules shall be inactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment shall be placed in secure containers. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

5.1.7 Physical Security Controls for End Entities

A subscriber shall physically protect any password or PIN that allows entry into the subscriber's digital certificate. Passwords or PINs should be memorized and not written down. If a password or PIN needs to be written down, it shall be stored in a locked file cabinet or container accessible only to designated personnel.

At no time shall subscribers leave their system unattended while the cryptographic module, or private key, is activated.

5.2 CA Procedural Controls

The CA's operating procedures must be documented and maintained to provide guidelines for secure and accurate operation of the facility. Accurate procedures detailing roles, responsibilities, and tasks must exist to control setup, changes and use of equipment, software and operating procedures. Reporting and response procedures must exist detailing points of contact and actions to be taken in the event of security incidents and malfunctions.

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. To ensure that one person acting alone cannot circumvent safeguards, CA responsibilities and authority shall be divided between multiple roles and individuals.

5.2.2 Number of Persons Required Per Task

The CA shall ensure that one person acting alone cannot circumvent safeguards.

5.2.3 Identification and Authentication for Each Role

Individuals shall identify and authenticate themselves before being permitted to perform any actions involved in a trusted role. User access shall be initiated and terminated

through a registration procedure. Accounts and passwords shall be issued and managed in a manner ensuring the integrity of the system. User rights and privileges must be limited to the duties and responsibilities of the individual to which they are issued. Users access rights shall be reviewed regularly. Policies regarding password length, complexity, and use shall be strictly adhered to.

5.3 Personnel Controls

The CA shall formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this Certificate Policy.

5.3.1 Personnel Security Controls for Certification Authorities

The individual assuming the role of CA Administrator should exhibit unquestionable loyalty, trustworthiness and integrity, and should demonstrate a high degree of security consciousness and awareness in their daily activities.

All CA personnel shall:

- Not be assigned duties that would interfere with their other responsibilities;
- Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Be appointed in writing by an approving authority;
- Have received proper training in the performance of their duties.

5.3.2 Clearance Procedures

Criminal background checks and clearance procedures are required for personnel filling positions where a high degree of trust is required. Clearance Procedures provide a mechanism for establishing and maintaining integrity and trust. Clearance procedures must be an ongoing process.

5.3.3 Training

CA employees must receive training in the organizational policies and operating procedures to ensure the CA's policies are adhered to. Training must be an ongoing and documented process. Refresher training will be required when the CSOS CA incurs significant system changes.

Personnel performing duties with respect to the operation of the CA shall receive:

- Training in the operation of the software and/or hardware used in the CSOS CA system;
- Training in the duties they are expected to perform;
- Briefing on stipulations of this CPS and the CP for CSOS PKI;
- Ongoing training in security procedures and policies.

5.3.4 Sanctions for Unauthorized Actions

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the CA, the CA, the OMA or the PMA may suspend his or her access to the CA system.

Breach of this CP or the CPS whether through negligence or with malicious intent, is subject to privilege revocation, administrative discipline, and/or criminal prosecution.

5.3.5 Employee Termination Controls

Once an employee holding a position of trust or any level of system access leaves the organization, their physical access and system access must be revoked upon receipt of termination documentation to ensure system integrity.

5.3.6 Contracting Personnel

Contractor personnel employed to operate any part of the CA are subject to the same background checks as US Government personnel, and shall be cleared to the level of the role performed.

5.3.7 Documentation Supplied to Personnel

The CP and relevant parts of the CPS shall be made available to the CA personnel and subscribers. Operation manuals shall be made available to CA personnel to facilitate the operation and maintenance of the CA.

5.3.8 Personnel Security Controls for End Entities

In addition to the CP and relevant parts of the CPS, subscribers shall be provided with information on the use and protection of the software used within the CSOS domain. The CA shall provide a technical help desk support for all subscribers.

Section 6 — Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The CA shall generate cryptographic keying materials using FIPS 140-2 level 3 validated cryptographic modules. The CA's key pair must be generated on a token in such a way that use of the private key at all times remains in control of the subscriber.

Subscriber signature key material for certificates issued by the CSOS CA shall, at a minimum, be generated using a FIPS 140-2 level 1 validated cryptographic module.

6.1.2 Private Key Delivery to Entity

Private keys shall not be transferred or exchanged. All entities generate their own private keys, and will not require delivery.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber's public key must be transferred to the CA in a way that ensures:

- It has not been altered during transit;
- The sender possesses the private key that corresponds to the transferred public key;
- The sender of the public key is the legitimate user claimed in the certificate application.

6.1.4 CA Public Key Delivery to Users

The public key of the CA signing key pair may be delivered to subscribers in an online transaction in accordance with IETF PKIX Part 3, PKCS 7 or via another appropriate mechanism. The CSOS CA shall post the certificate it issues in the CA repository.

6.1.5 Key Sizes

CSOS CA keys shall use at least 2048 bit RSA with Secure Hash Algorithm version 1 (SHA-1) in accordance with FIPS 186-2.

CSOS subscriber keys must be at least 1024 bits with a FIPS 186-2 compliant hash function.

6.1.6 Public Key Parameters Generation

Public key parameters prescribed in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186-2.

6.1.7 Parameter Quality Checking

Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186-2.

6.1.8 Hardware/Software Key Generation

The CSOS CA key generation shall be performed solely in hardware. At a minimum, the generation process for the CSOS CA shall be FIPS 140-2 Level 3 compliant.

At a minimum, the generation process for subscribers shall be FIPS 140-2 Level 1 compliant and shall be generated in the client's system.

6.1.9 Key Usage Purposes (as per X.509 v3 key usage field)

Subscriber signing keys must be used for digital signature and non-repudiation; CA signing keys may also be used for certificate and CRL signing.

6.2 Private Key Protection

The CA and subscriber must take adequate steps to protect their private keys in accordance with this Certificate Policy.

6.2.1 Standards for Cryptographic Module

At a minimum, CA cryptographic modules must be validated to FIPS 140-2 level 3.

At a minimum, subscriber cryptographic modules must be validated to FIPS 140-2 level 1.

6.2.2 Private Key (n out of m) Multi-Person Control

A minimum of two persons shall be required for all CA operations activities.

6.2.3 Private Key Escrow

Escrow of private digital signature keys, either CA or subscriber, by an external third party is prohibited.

6.2.4 Private Key Backup

The CA private keys shall be backed up. All copies of the backed-up key must be handled in an accountable manner that protects it from unauthorized access and unauthorized use.

Backup of the subscriber's private key is prohibited.

6.2.5 Private Key Archival

Subscriber private signature keys shall not be archived, escrowed, or copied. See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Entry into Cryptographic Module

The CA signing private key pair shall be generated and handled by the CA cryptographic module in a manner compliant with FIPS 140-2 level 3.

6.2.7 Method of Activating Private Key

Authorized personnel shall activate CA private signing keys in accordance with Section 5.2.2. The means of authentication must be biometrics.

The subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Approved means of authentication include pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.8 Method of Deactivating Private Key

CA private signing keys shall be deactivated either through a manual logout process or automatically after a period of inactivity as defined in the CPS.

If a cryptographic module is used to store the subscriber's private key, then the cryptographic module that has been activated shall not be left unattended or otherwise available to unauthorized access. After use, the cryptographic module shall be deactivated (e.g., via a manual logout procedure, or automatically after a period of inactivity). If a hardware cryptographic module is used, it shall be maintained under the control of the subscriber.

6.2.9 Method of Destroying Private Key

The method for destroying the CA's private key shall be defined in the CPS. The method of destruction must be approved by the PMA.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CSOS CA Public Key shall be archived in accordance with the procedures described in Section 4.6 of the CPS.

6.3.2 Usage Periods for the Public and Private Keys

CA certificates shall have a validity period of 10 years.

Subscriber certificates shall expire upon the expiration of the subscriber's DEA registration. Subscribers must renew their CSOS Certificate to continue to conduct CSOS business electronically.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data (password) used to unlock the CA or subscriber private keys, in conjunction with any other access control, shall be generated in conformance with FIPS-112 and shall result in a high level of strength for the keys or data to be protected. For the CA, it shall satisfy the policy-enforced at/by the cryptographic module.

6.4.2 Activation Data Protection

Activation data used to unlock the CA or subscriber private key shall be securely protected against modification and disclosure. Activation data for private keys associated with certificates asserting individual identities shall never be shared. The protection mechanisms for the CA shall be described in the CPS.

6.5 CA Computer Security Controls

The CA computer security controls must be outlined in the CA security policy. The operating system shall enforce the identification, authentication, auditing, and separation of roles of all users. A secure logon process shall be used to access the CA's systems. An access control policy and an account management process shall be implemented to restrict access to information and system functions. Isolation of sensitive systems to a dedicated computing environment is required. Terminal identification shall be used to authenticate connections. Inactivity timeouts on terminal sessions and restrictions on connection times for high-risk applications shall be implemented to prevent unauthorized access to enhance security.

Malicious software detection and prevention controls must be implemented and must be kept current. This is an ongoing task. Procedures must exist to address prevention, removal and recovery.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

New equipment and software, including patches and updates, must be thoroughly tested on a separate platform for functionality and vulnerabilities prior to being implemented on operational systems. Operational systems must be physically and logically separate from developmental systems and systems used for testing software patches and updates to maintain integrity of services provided. Procedures for implementation on operational systems will be developed during testing on isolated systems.

6.6.2 Security Management Controls

A security policy document must exist. This document must provide guidance facilitating the secure operation of the CA and ensuring the integrity of its operating environment. Responsible individuals will implement and maintain the security policy.

6.7 Network Security Controls

Access to unused ports and services must be denied to prevent misuse. Users shall be provided access only to services that they are specifically authorized to use from terminals designated for that function. Connections to services from network paths other than those specified for that function must be refused. Remote access and connections from remote computers must be authenticated. External threats shall be mitigated by controls such as firewalls, network intrusion detection systems and router access lists to protect the internal network. The CA shall document security attributes of all network services.

6.8 Cryptographic Module Engineering Controls

Requirements for cryptographic modules are as stated in Section 6.1.

Section 7 — Certificate and CRL Profiles

7.1 Certificate Profile

The CA certificate shall be issued in the X.509 format, and will include a reference to the OID for this Certificate Policy within the Certificate Policies field. Supported certificate extensions shall be identified in the CSOS CPS.

7.1.1 Version Number

The CA shall issue X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions shall include the extensions specified in the Minimum Interoperability Specification for PKI Components.

7.1.3 Algorithm Object Identifiers

At a minimum the following algorithm must be used and/or supported by the CA and End-Entities for signing and verification:

Algorithm	Object Identifier	Issuing Authority
sha1WithRSAEncryption	1 2 840 113549 1 1 5	RSADSI

7.1.4 Name Forms

In a certificate, the issuer DN and subject DN fields shall contain the full X.500 Distinguished Name of the CA.

7.1.5 Name Constraints

Subject and Issuer DNs must comply with CSOS standards and be present in all certificates.

7.1.6 Certificate Policy Object Identifier

The CA must ensure that the CSOS Certificate Policy OID is contained within the certificates.

7.1.7 Usage of Policy Constraints Extension

N/A

7.1.8 Policy Qualifiers Syntax and Semantics

The CA must populate the policyQualifiers extension with the URI of its CP.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The CA issuing certificates under this Certificate Policy shall mark the Certificate Policy extension as critical. Critical extensions shall be interpreted as defined in PKIX.

7.2 CRL Profile

7.2.1 Version number(s)

The CA shall issue X.509 version 2 CRLs in accordance with the *CSOS Certificate and CRL Profile* document.

7.2.2 CRL and CRL entry extensions

All Entity PKI software must correctly process all CRL extensions identified in the *CSOS Certificate and CRL Profile* document. CRLs shall be issued in a format that is consistent with the Minimum Interoperability Specification for PKI Components.

Section 8 — Specification Administration

8.1 Specification Change Procedures

The PMA shall review this CP at least once every year. Errors, updates, or suggested changes to this CP shall be communicated to CSOS subscribers. All policy changes under consideration by the PMA shall be disseminated to interested parties. All interested parties shall provide their comments to the PMA in a fashion to be prescribed by the PMA.

8.2 Publication and Notification Policies

Only editorial changes or typographical corrections may be made to this specification without notification. Any item in this Certificate Policy may be changed with 90 days notice. Changes to items, which will not materially impact a substantial majority of relying parties using this Certificate Policy, may be changed with 30 days notice.

8.3 CPS Approval Procedures

The PMA shall make the determination that a CPS complies with this policy.

Section 9 — Glossary

Access Control Process of granting access to information only to authorized users, programs, processes, or other systems.

Activation Data Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).

Archive Long-term, physically separate storage.

Audit Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Data Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.

Authenticate To confirm the identity of an entity when that identity is presented.

Authentication Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

Authority Revocation List (ARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioral characteristic of a human being such as a fingerprint.
Certificate	(Subscriber) certificates identify the individual named in the certificate, bind that person to a particular public/private key pair, and provide sufficient information demonstrating the subscriber is operating under the authority of the DEA CSOS program.
Certificate Policy (CP)	A "named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements" [X.509]. The CSOS Certificate Policy specifies (1) the Certification Authorities, the Subscribers, and the Relying Parties authorized to participate in the PKI program described by this Policy, (2) the obligations of the participants governed by this Certificate Policy, and (3) the minimum requirements for the issuance and management of digital certificates used within the CSOS program and other suitable applications.
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certification Authority (CA)	This term is used to identify the Root CA role operated by DEA.

CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certification Practices Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific CP requirements.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Cryptographic Module	Set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Drug Enforcement Agency (DEA)	The DEA regulates the manufacture and distribution of controlled substances in the United States.
End Entity	Relying Parties and Subscribers.
Federal Information Processing Standards (FIPS)	These are Federal standards that prescribe specified performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc.

Firewall	Gateway that limits access between networks in accordance with local security policy.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge Property or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Internet Engineering Task Force (IETF)	A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the architecture and the smooth operation of the Internet.
Key Changeover	The procedure used to change CA keys.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key Pair	Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.

Object Identifier (OID)	An alphanumeric number registered with an internationally recognized standards organization used within PKI to uniquely identify policies and supported cryptographic algorithms.
Operations Management Authority (OMA)	Parties responsible for managing all personnel and activities involved in the day-to-day operations of the Certificate Authority, Registration Authority and Help Desk.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Registration Authority (RA)	CAs that process the registration of subscribers and operate according to the stipulations of a Certificate Policy.
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A relying party is the entity who, by using a subscriber's certificate to verify the integrity of a digitally signed message, identifies the creator of a message, and relies on the validity of the public key bound to the subscriber's name. The relying party is responsible for checking the validity of the certificate by checking the appropriate certificate status information. The relying party must use the certificate to verify the integrity of a digitally signed message and to identify the creator of a transaction.
Renewal of certificates	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Root CA	The CSOS Root CA will operate in accordance with the provisions of its Certification Practices Statement. The CSOS Root CA will also perform the following functions: (1) accept and process

	applications for operations from Subordinate CAs; (2) issue certificates to Subordinate Certificate Authorities approved by the PMA; (3) publish Subordinate CA certificate status information.
Server	A system entity that provides a service in response to requests from clients.
Subordinate CA	A Subordinate CA is an entity authorized by the PMA to create, sign, and issue public key certificates to authorized subscribers.
Subscriber	A subscriber is the entity whose name appears as the subject in a certificate issued by the CA, who attests that it uses its key and certificate in accordance with the Certificate Policy asserted in the certificate. CSOS subscribers are limited to DEA registrants and agents of registrants as stipulated in the Code of Federal Regulations (CFR) §1301.22.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Trusted Role	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.
Vulnerability Assessments	Vulnerability assessments are conducted to identify potential vulnerabilities or events that would affect the integrity and operation of the CA.